Amendments to the Claims

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Previously presented)A method of communicating a communication fragment, the communication fragment comprising a target group address referring to at least two receiver devices, the method comprising acts of:

a sender device adding a cryptographic message integrity code forming a protected communication fragment to protect at least part of the communication fragment, wherein the cryptographic message integrity code is at least partly based on the target group address;

the sender device transmitting the protected communication fragment to at least one receiver device through use of a router device that is not part of a trusted group to which the sender device and the at least one receiver device belong;

the router device, for the at least one receiver device referred to in the target group address, replacing the target group address with an address of the at least one receiver device forming a modified protected communication fragment, while maintaining the unchanged cryptograph message integrity code, and subsequently forwarding the modified protected communication fragment to the at least one receiver device;

the at least one receiver device receiving the modified protected communication fragment; and

the at least one receiver device restoring the original protected communication fragment by replacing the address of the at least one receiver device with the target group address to allow verification of the protected communication fragment using the message integrity code.

2. (Previously presented)The method according to claim 1, wherein the communication fragment comprises a bit field IA to indicate whether indirect addressing is used.

3. (Previously presented) The method according to claim 1, comprising an act of sharing with the sender device and the at least one receiver device, a common cryptographic key which is not shared with the router, and where the cryptographic message integrity code is computable and verifiable only by using the common cryptographic key.

4. (Previously presented) The method according to claim 3, wherein the common cryptographic key is used to encrypt the message content.

5. (Previously presented) The method according to claim 1, wherein the act of restoring the protected communication fragment comprises an act of replacing the address of the at least one receiver device with each of a plurality of group identities that include the sender device to determine which of the plurality of group identities the message integrity code matches.

6. (Previously presented) The method according to claim 1, wherein the act of replacing the target group address comprises an act of storing the target group address in the modified protected communication fragment, and

wherein the act of restoring the original protected communication fragment comprises an act of restoring the protected communication fragment using the stored first target address reference in the modified protected communication fragment in order to allow verification of the message integrity code.

7. (Previously presented) A sender device being arranged to transmit a communication fragment through a router device towards a receiver device, the communication fragment comprising a target group address referring to at least two receiver devices, the sender device comprising:

protecting means being arranged to add a cryptographic

message integrity code to protect at least part of the communication fragment, wherein the cryptographic message integrity code is at least partly based on the target group address and a cryptographic key; and

transmitting means being arranged to transmit the communication fragment to a receiver device through a router device that is not able to modify the cryptographic message integrity code, that does not have access to the cryptographic key, and that is not part of a trusted group to which the sender device and the at least two receiver devices belong.

8. (Previously presented) A router device being arranged to route a communication fragment from a sender device towards a receiver device, the communication fragment comprising a target group address referring to at least two receiver devices, the router device comprising:

receiving means being arranged to receive the communication fragment comprising a cryptographic message integrity code that is at least partly based on the target group address;

modifying means being arranged to modify the communication fragment, by replacing the target group address by a reference referring to one of the at least two receiver devices, while maintaining the original cryptographic message integrity code without use of a cryptographic key related to the cryptographic message integrity code and without being a part of a trusted group to which the sender device and the at least one receiver device belong; and

transmitting means being arranged to transmit the modified communication fragment to the one of the at least two receiver devices.

9. (Previously presented) A receiver device being arranged to receive a modified communication fragment originating from a transmitter device through a router device, the modified communication fragment being derived from a communication fragment comprising a target group address referring to at least

two receiver devices, the receiver device comprising:

receiving means being arranged to receive the modified communication fragment sent by the transmitter device through the router device, wherein the router device is not part of a trusted group to which the transmitter device and the at least two receiver devices belong;

restoring means being arranged to restore the communication fragment that was used to compute a cryptographic message integrity code included in the modified communication fragment that is at least partly based on the target group address by replacing an address of the receiver device with the target group address; and

verification means being arranged to verify the cryptographic message integrity code.

10-11. (Canceled)

12. (Previously presented) The receiver device according to claim 9, wherein the transmitter device and the receiver device share a common cryptographic key which is not shared with the router, and where the cryptographic message integrity code is computable and verifiable only by using the common cryptographic key.

13. (Previously presented) The receiver device according to claim 12, wherein the common cryptographic key is used to encrypt the message content.

14. (Previously presented) The receiver device according to claim 9, wherein the receiver device is arranged to restore the communication fragment by replacing the address of the receiver device with each of a plurality of group identities that include the transmitter device to determine which of the plurality of group identities the cryptographic message integrity code matches.